Remarks

In the Office Action dated October 13, 2004, the Examiner withdrew his previous rejections after finding Applicants arguments of non-anticipation and non-obviousness persuasive. However, also in the Office Action, the Examiner presented a new rejection claims 1-39 based on a newly cited reference.

The Examiner rejected claims 1-39 as anticipated by Minear, et al. (U.S. Patent No. 5,983,350) under 35 U.S.C. 102(e). Applicants submit that Minear does not disclose all the elements of Applicants' claimed invention.

As an initial matter, it is important to keep in mind that all of the pending claims recite distributed network address translation (DNAT) with security. For example, Claim 1 of the present application recites "requesting ... one or more locally unique security values from a second network device ... for distributed network address translation with security."

The present invention can be useful for solving security problems associated with network address translation. This was noted in the background section of the present application.

> There are several problems associated with using current versions of NAT when security is required and the IPSEC protocol is used. Current versions of NAT violate certain specific principles of the IPSEC protocol that allow establishment and maintenance of secure end-to-end connections of an IP network.
>
> A NAT router typically needs to modify an IP packet (e.g., network ports, etc.). However, once an IP packet is protected by IPSEC, it must not be modified anywhere along a path from an IPSEC source to an IPSEC destination. Most NAT routers violate IPSEC by modifying, or attempting to modify individual IP packets.
>
> Even if a NAT router does not modify data packets it forwards, it must be able to read network port numbers (e.g., TCP, UDP, etc.) in the data packets. If certain IPSEC features are used (e.g., Encapsulated Security Payload ("ESP")), the

> network port numbers are encrypted, so the NAT router typically will not be able to use the network ports for NAT mapping.
>
> Local host network devices on a Local Area Network ("LAN") that use NAT typically possess only local, non-unique IP addresses. The local non-unique IP addresses do not comprise a name space that is suitable for binding an encryption key (e.g., a public key) to a unique entity. Without this unique binding, it is not possible to provide necessary authentication for establishment of Security Associations. Without authentication, an endpoint of a connection cannot be certain of the identity of another endpoint, and thus cannot establish a secure and trusted connection.

Patent Application, p. 5, ln. 19 to p. 8, ln. 9.

DNAT allows a single routable IP address may be multiplexed among several hosts on a local stub network, none of which have a globally routable IP address. Thus, for example, DNAT is useful for extending the lifetime of IP-4 systems. Additionally, DNAT allows routers to perform the required address mapping without modifying the contents of the routed packets. (i.e., TCP/UDP header, or payload). Further, the present invention provides for distributed network address translation using Internet Protocol security in a way that does not significantly increase a burden on the routers or other network devices that provides network address translation.

Minear does not teach DNAT. In fact, Minear does not teach network translation in any form. In contrast with the each claim of the present application, Minear simply teaches a system for determining, at the IP layer, if a message is encrypted, and, if the message is encrypted, decrypting the message and passing the decrypted message up the network protocol stack to the application level proxy. (Minear, Abstract).

The differences between Minear and the present invention continue. For example, contrary to independent claims 1, 9, 34, and 36 Minear fails to disclose requesting or receiving "locally unique security values" from a second network device on the same computer network to uniquely identify the first network device.[1]

Next, claims 3, 11, 31, and 37 contain the limitation of the second network device being a distributed network address translation (DNAT) router. A DNAT router is used to allocate "locally unique security values that are used as the Internet Protocol security protocol security parameters indexes. A router used for distributed network address translation is also used as a local certificate authority that may vouch for identities of local network devices, allowing local network devices to bind a public key to a security name space." Patent Application, Summary of Invention.

Minear does even explicitly disclose a router. Moreover, Minear does not even implicitly provide for a router that exhibits any of the functionality associated with the above described DNAT router. <u>Minear simply does not disclose DNAT routers of claims 3, 11, 31, and 37.</u>

Minear does not teach each and every element in any of the claims. Thus, its use as an anticipatory reference is improper and must be withdrawn.

[1] Claims 7, 20, 28, 34, and 36 refer to "locally unique ports" which are likewise not disclosed by Minear.

Conclusion

In view of the foregoing, Applicants respectfully submit that all of the presently pending claims are now in condition for allowance, and Applicants respectfully request prompt favorable reconsideration.

Respectfully submitted,

Date: JAN 12, 2008

By:
Dennis D. Crouch
Registration No. 55,091